UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,504	11/26/2003	Franck Le	800.0186.U1(US)	6168

29683 7590 11/03/2010

HARRINGTON & SMITH
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2491	
MAIL DATE	DELIVERY MODE
11/03/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,504	LE ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2491	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,11-15,18,42,43,50-56,59,60,63,64 and 66-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,11-15,18,42,43,50-56,59,60,63,64 and 66-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/26/2003* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 9/13/2010.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/23/2010 has been entered.

Response to Arguments

Applicant's arguments filed 8/23/2010 have been fully considered but they are moot in view of the new grounds of rejection presented below.

Regarding the applicants' argument that Mitreuter teaches away from including an address in a database of a server…in a packet, the examiner does not find the argument persuasive. Simply because Mitreuter teaches including the entire certificate in the packet, does not result in teaching away from replacing the entire certificate with a URL where the entire certificate can be retrieved. The teachings of Mitreuter were simply its preferred embodiment, not a teaching away from any changes. Also note the teachings of Song below, which shows that including a URL where a public key can be downloaded from in a transmission is an alternative to including the public key itself in the transmission. As such, the examiner does not find the argument persuasive.

All objections and rejections not set forth below have been withdrawn.

Claims 1,2,4,11-15,18,42,43,50-56,59,60,63-64 and 66-68 have been examined.

Claim Rejections - 35 USC § 103

Claims 1-2, 11, 15, 18, 42-43, 50, 54-56, 59-60, and 63-64, and 66-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (US Patent Number 6,389,532) hereinafter referred to as Gupta, and further in view of Mitreuter et al. (US Patent Application Publication 20030033375) hereinafter referred to as Mitreuter, and further in view of Song et al. (US Patent Application Publication 20030065947) hereinafter referred to as Song.

Regarding claim 1, Gupta disclosed a method (See Gupta Fig. 1 Element 104, 108 or 112), comprising the steps of: generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4), wherein the validity information comprises all necessary information required to perform a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); the validity information comprising algorithm information to be used for performing the validity check of the packet and no pre-established security association is needed to verify the packet and algorithm initialization information(See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); generating a packet header (302), comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4) ; and sending the packet including the packet header from a first network node to a second network node (See Gupta Col. 6 Paragraph 4), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in

order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claim 18, Gupta disclosed an apparatus comprising: validity information generating means for generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); packet header generating means for generating a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and sending means for sending the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2) and the validity information comprises algorithm information to be used for performing the validity check of the

packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claim 42, Gupta disclosed an apparatus, comprising: a validity information generator configured to generate validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); a packet header generator configured to generate a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and a transmitter configured to send the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the

linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claim 55, Gupta disclosed an apparatus, comprising: a receiver configured to receive packets from a sending network node (See Gupta Fig. 1 Element 108, Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of

a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claim 59, Gupta disclosed an apparatus, comprising: a transmitter configured to forward packets from a sending network node to a receiving network node (See Gupta Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to

perform a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the

packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claims 63 and 67, Gupta disclosed a method comprising: receiving packets (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); and performing a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the

linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claim 64, Gupta disclosed a method comprising: forwarding received packets (Gupta Col. 7 Paragraph 2); and performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet (Gupta Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claim 66, Gupta disclosed a computer readable storage medium comprising a computer program (See Gupta Fig. 1 Element 104, 108 or 112), that when executed controls a processor to perform: generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4), wherein the validity information comprises all necessary information required to perform a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); the validity information comprising algorithm information to be used for performing the validity check of the packet and no pre-established security association is needed

to verify the packet and algorithm initialization information(See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); generating a packet header (302), comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4) ; and sending the packet including the packet header from a first network node to a second network node (See Gupta Col. 6 Paragraph 4), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claim 68, Gupta disclosed a computer readable storage medium comprising a computer program (See Gupta Fig. 1 Element 104, 108 or 112), that when executed controls a processor to perform: forwarding received packets (Gupta Col. 7 Paragraph 2); and performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet (Gupta Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2), wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example), but Gupta failed to specifically teach the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained.

Mitreuter teaches that in an analogous art for generating and signing packets, the public key certificate containing the public key of the sender can be included in the packet header in order to allow the packet signature to be readily verified by the recipient of the packet (Mitreuter Paragraph 0037).

Song teaches that in a transmission system, alternative to including the entire public key of the sender in a transmission, a linking address can be included in the transmission, and the linking address is used to download the public key from the registry server (Song Paragraph 0142).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mitreuter and Song in the packet verification system of Gupta by including a linking address to the public key certificate including the public key used to verify the packet signature in the packet header. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow any recipient of the packet to readily verify the signature of the packet without the increased burden on the sender of transmitting the entire certificate for each packet.

Regarding claims 2, 43, 56 and 60, Gupta, Mitreuter, and Song disclosed that the generating of the validity information comprises generating security information indicating security services applied to the packet (See Gupta Col. 5 Paragraph 7).

Regarding claims 11 and 50, Gupta, Mitreuter, and Song disclosed that the generating of the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4).

Regarding claim 15 and 54, Gupta, Mitreuter, and Song disclosed signing the packet using a private key corresponding to the public key indicated by the validity information in the packet header in a sending network node (See Gupta Col. 6 Paragraph 4 and Mitreuter Paragraph 0037).

Claims 4, 12-14, and 51-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta, Mitreuter, and Song as applied to claims 1 and 42 above, and further in view of Naudus (US Patent Number 6,202,081).

Regarding claims 12-14, and 51-53, Gupta, Mitreuter, and Song disclosed validation of packets, but failed to disclose that the step of generating the validity information comprises generating an information item for preventing replay attacks.

Naudus teaches that in a packet filtering system, packets should include timestamps in order to prevent replay attacks. Naudus further teaches that "[r]eplay attacks occur when a malicious user gains access to a router or other network device on a computer network that is forwarding data packets. Legitimate data packets are intercepted and then re-sent at a later time to allow the malicious user to appear as a legitimate user. A firewall helps prevent replay attacks by checking a time-stamp in the data packet that prevents the data packets from being re-sent at a later time." (See Naudus Col. 2 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Naudus in the packet validity checking system of Gupta, Mitreuter, and Song by including a timestamp in each packet and verifying the timestamp at the validity checker. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent replay attacks in the network. In this combination, the inclusion of a timestamp in each packet, in itself, is an indication of a procedure to be used for anti replay attacks.

Regarding claim 4, Gupta, Mitreuter, and Song did not specifically teach that the step of generating the algorithm information comprises generating the algorithm information which indicates an algorithm to be used for performing the validity check of the packet. However, as taught by Naudus, in Col. 6 Line 60 - Col. 7 Line 7, it is well known to include in the packet header, an identification of which algorithm was used to sign the packet. As such, it would have

been obvious to have included this information within the packet. Furthermore, the ordinary person skilled in the art at the time of invention would have recognized that this would allow for the use of a multiplicity of signature algorithms, as well as allowing updating of the signature algorithms in the future, and therefore it would have been obvious to have included an indication of the signature algorithm in the packet.

Claims 11, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta and Mitreuter as applied to claims 6 and 23 above, and further in view of Nikander (US Patent Number 7,155,500).

Gupta and Mitreuter disclosed including public key information within the packets, including the public key itself within the packets, but failed to specifically disclose that the step of generating the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node. Gupta did disclose that the public and private key pairs can be generated and stored in a certification server (See Col. 4 Paragraph 2).

Nikander teaches that by including the certificate of the public key, the receiving host can verify that the public key is truly owned by the sender (See Nikander Col. 10 Line 50 – Col. 12 Line 9).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Nikander in the packet verification system of Gupta and Mitreuter by including the public key certificate within each packet and verifying that the sender of each packet owned the public key used to sign the packet. This would have been obvious

because the ordinary person skilled in the art would have been motivated to ensure that a malicious node was not claiming to be a different node.

Conclusion

Claims *1,2,4,11-15,18,42,43,50-56,59,60,63-64 and 66-68* have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok Patel can be reached on (571)272-3972. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Primary Examiner, Art Unit 2491